Cyber Incident Annex – State of Wisconsin

Wisconsin Coordinating Agencies:

Department of Administration / Division of Enterprise Technology (DOA/DET)
Department of Military Affairs / Division of Emergency Management (DMA/WEM)

Wisconsin Cooperating Agencies:

Department of Military Affairs / Wisconsin National Guard (DMA/WI NG)
Department of Justice / Wisconsin Statewide Information Center (DOJ/WSIC)

Federal Cooperating Agencies:

Department of Homeland Security (DHS) .
Department of Justice / Federal Bureau of Investigation (DOJ/FBI)
Department of Defense (DoD)

Note: The Wisconsin Cyber Incident Annex is based on:
1) National Response Framework (NRF)/Cyber Incident Annex (CIA) dated January 2008.Where appropriate sections of the NRF/CIA are quoted and shown in italics.
2) National Cyber Incident Response Plan Draft Version 1.2

I. INTRODUCTION

A. Purpose:

1. This Annex discusses policies, organization, actions, and responsibilities for a coordinated, multidisciplinary, broad-based approach to prepare for, respond to, and recover from cyber-related incidents.

2. These may be either statewide or national cyber incidents impacting critical processes or economic activity.[1]

B. Scope:

1. This Annex describes the framework for Wisconsin State Agencies to support local units of government during a cyber incident response. This support is coordinated with State and Federal agencies. Wisconsin is a "Home Rule" state and "the role of any state agency, including the department of military affairs and the division, in an emergency declared under this chapter, is to assist local units of government and local law

[1] The U.S. National Response Plan term "Incident of National Significance" was eliminated with the publication of the National Response Framework.

enforcement agencies in responding to a disaster or the imminent threat of a disaster.[2]"

2. The coordination with the Federal Government is dynamic and shaped by the nature of the event. For example a cyber incident impacting a Wisconsin airport would involve the Department of Transportation, a Wisconsin power plant the Department of Energy, or a sovereign Indian Tribe in Wisconsin the Department of Interior. The complexity of a Cyber Annex that attempted to lay out the possible permutations and combinations of Federal / State relations would hobble both the usefulness and maintainability of the document.

3. This Annex is intended to develop broad concepts has focused on Wisconsin's interface with three principal Federal Agencies. They are:

   - DHS. Office of Cybersecurity and Communications. Which includes: National Communications System, National Cybersecurity Division, Office of Emergency Communications, the NCS' National Coordinating Center (NCC) for communications, NCSD's United States Computer Emergency Readiness Team (U.S.-CERT).

   - DoD. The DoD Cyber Crime Center (DC3), U.S. Strategic Command and the subordinate U.S. Cyber Command.

   - DOJ/FBI

4. A cyber incident will not be bounded by Lake Michigan or the Mississippi river and may lack an easily identifiable signature. Cyber incidents alone, or in combination with other events, will present new and unique challenges to the Wisconsin emergency management community.

5. Wisconsin's Cyber Annex foundational authority is Wisconsin Executive Order #81 which designates the National Incident Management System (NIMS) as the basis for incident management in the State of Wisconsin. Due to the unique aspects of a cyber incident of statewide or national significance an effective Unified Command is required. The National Incident Management System (NIMS)[3] defines the elements of unified command as:

   - Developing a single set of objectives;

   - Using a collective, strategic approach;

[2] Wisc. Stat. § 323.01 (2)

[3] U.S. Department of Homeland Security, The National Incident Management System is available at the NRF Resource Center, http://www.fema.gov/NRF.

- Improving information flow and coordination;
- Creating common understanding of joint priorities and restrictions;
- Ensuring that no agency's legal authorities are compromised or neglected; and
- Optimizing the combined efforts of all agencies under a single plan.

6. Wisconsin emergency managers working with public and private partners will bring to bear critical skills required to take immediate action in identifying, responding to and recovering from a cyber incident. These skills include:

- Planning
- Hazard Identification
- Direction, Control and Coordination
- Laws and Authorities
- Exercise, Evaluations & Corrective Actions
- Communications and Warnings
- Hazard Mitigation
- Resource Management
- Continuity of Operations/Continuity of Government
- Mutual Aid

7. The Wisconsin Cyber Annex is built on the premise that the following partners will work together to form a NIMS Unified Command to coordinate the actions necessary for rapid identification, information exchange, response, and remediation to mitigate the damage caused by a cyber event:

- DOA/DET
- DMA/WING
- Law enforcement

- Technology resources from the private and public sectors.

8. This framework may be utilized in any incident with cyber-related issues, including significant cyber threats and disruptions; crippling cyber attacks against the Internet or critical infrastructure information systems; technological emergencies; or declared disasters.

9. This Annex describes the specialized application of the National Response Framework (NRF) to cyber-related incidents. These cyber incidents may result in activation of the Cyber Annex and other Emergency Support Function (ESF) annexes. When processes in multiple annexes are activated, DMA/WEM continues its responsibilities under this Annex and also fulfills its responsibilities as described in other annexes to the Wisconsin Emergency Operations Plan.

C. Policies

1. The procedures discussed in this Annex are governed by Federal and State Laws, policies and practice. Also, reports and studies provide a framework for cyber incident planning. The foundational documents listed in Appendix B: Authorities illustrate that a cyber incident has the potential to impact all aspects of civil and economic matters. These documents also demonstrate that policy makers at the Federal and State level have recognized cyber incident risks for over 20 years. Yet there is not a unified policy today for cyber incidents.

2. DHS has published in draft form the National Cyber Incident Response Plan (NCIRP.) "The purpose of the NCIRP is to establish a high-level National plan that details the organizational roles, responsibilities, and actions to prepare for, respond to, and begin to recover from a Cyber Incident. It ties various policies and doctrine together into a single, tailored, strategic, cyber-specific plan designed to assist with operational planning and exercises and to guide national-level incident response and short-term recovery efforts." The draft includes:

   - DHS National Cybersecurity and Communications Integration Center: The NCCIC is a 24x7x365 integrated cybersecurity and communications operations center. It serves as a centralized location where the operational elements involved in communications and cyber response activities are physically and virtually collocated.

   - The Multi-State Information Sharing and Analysis Center (MS-ISAC) is identified as a key resource for State, local, tribal and territorial government information sharing, early warnings and alerts, mitigation strategies, training, exercises and to ensure that overall cyber situational awareness is maintained.

- Private sector is incorporated in two primary groups that play a role in "steady state" cybersecurity activities:
    - CIKR owners and operators; and
    - The general private sector ("Private Sector").
- The Unified Coordination Group (UCG) works during "steady state" to ensure unity of NCCIC preparedness efforts and to facilitate the rapid response to a Cyber Incident. It is composed of Senior Officials and Staff that have been pre-selected by their department, agency, or organization.

3. This document is not intended to establish a cyber policy; but, rather build on fundamental policy principles and describe how organizations work collaboratively concerning cyber incidents. These principles are:

- Wisconsin is a "Home Rule" State.
- The citizens of Wisconsin expect a cyber response to effectively coordinate available assets and tools through preparation, response, mitigation and recovery from a cyber incident.
- NIMS and NRF are adaptable to cyber incidents.

II. CONCEPTS OF OPERATIONS

A. General

1. A cyber-related incident may take many forms: an organized cyber attack, an uncontrolled exploit such as a virus or worm, a natural disaster with significant cyber consequences, or other incidents capable of causing extensive damage to critical infrastructure or key assets. In the event of a cyber-related incident, or disaster with a cyber component, it should be reported to DOJ/WSIC and one or more of the agencies listed in Appendix A.

2. Large-scale cyber incidents may overwhelm government and private-sector resources by disrupting the Internet and/or taxing critical infrastructure information systems. Complications from disruptions of this magnitude may threaten lives, property, the economy, and national security. Rapid identification, information exchange, investigation, and coordinated response and remediation are critical in cyber consequence management.

3. The Federal Government plays a significant role in managing intergovernmental (Federal, State, local, and tribal) and, where appropriate, public-private coordination in response to a cyber incident. Responsibilities include:

   - Providing indications and warning of potential threats, incidents, and attacks;
   - Information-sharing both inside and outside the government, including best practices, investigative information, coordination of incident response, and incident mitigation;
   - Analyzing cyber vulnerabilities, exploits, and attack methodologies;
   - Providing technical assistance;
   - Conducting investigations, forensics analysis, and prosecution;
   - Attributing the source of cyber attacks;
   - Defending against the attack; and
   - Leading national-level recovery efforts.

4. These activities are the product of, and require, a concerted effort by Federal, State, local, and tribal governments, and nongovernmental entities such as private industry and academia.

5. The Federal Government supports the State Government's efforts to provide on-going support to local and tribal governments. Pre-incident planning and coordination for a cyber incident is critical as the actual cyber incident may significantly degrade or destroy communications. The Wisconsin Cyber Annex follows the National Response Framework (NRF)[4] and the overview of incident annexes provided in the previously published National Response Plan (NRP)[5].

6. Not all national level cyber incidents will have statewide significance. Likewise a statewide incident may not have national significance. Statewide cyber incidents are:

   - Declaration by the Governor under the provisions of Wis. Stats. Chapter 323.

[4] U.S. Department of Homeland Security. National Response Framework, P78, January 2008.

[5] U.S. Department of Homeland Security, National Response Plan, Page INC-I, December 2004

- Authoritative reports of the successful targeting of Wisconsin's information infrastructure for exploitation, disruption, or destruction. This infrastructure includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.

- Authoritative reports of a cyber incident, either intentional or unintentional, that threatens Wisconsin's economic prosperity through a loss of integrity of the communications and information infrastructure.

Specific responsibilities identified in this Annex are:

7. DMA/WEM:

   - Conduit with the Federal Emergency Management Agency (FEMA).
   - Responding to incidents through operation of the State Emergency Operations Center
   - Facilitating the coordination of recovery efforts.
   - Facilitating communications with other emergency entities involved in cyber incidents on a statewide basis.
   - Coordination of training and education programs

8. DOJ/WSIC:

   - Threat information-sharing both inside and outside the government, including best practices, investigative information, coordination of incident response, and incident mitigation;
   - Assist in attributing the source of cyber attacks through DOJ resources and the network of fusion centers;
   - Forensic analysis and support provided by WISC and DCI staff;
   - Provide a top down conduit for information from the U.S. Department of Justice and U.S. Department of Homeland Security to Wisconsin State Government; and,
   - Provide a bottom up conduit to DOJ and DHS for information from the Threat Liaison Officers and others..

9. DOA/DET:

- Conduit with the United States Computer Emergency Response Team (US-CERT) and the Multi-State Information Sharing and Analysis Center (MS-ISAC).
- Analyzing cyber vulnerabilities, exploits, and attack methodologies;
- Providing technical assistance;
- Defending against an attack; and
- Providing indications and warning of potential threats, incidents, and attacks;

10. DMA/WING:

- Computer Network Defense. Within law, DoD policy and practice the DMA/WING may provide information assurance best practices, vulnerability assessment exercises, penetration testing and intrusion detection. The DMA/WING's Computer Network Defense Team has the capabilities to provide:
- Cyber Analysis capabilities include forensic examination of networks and systems;
- Threat assessment and unclassified adversary tactics, techniques, and procedures;
- Situation Awareness/Information Sharing;
- Incident mitigation;
- Incident Recovery; and,
- Training and Education.

11. The key to Wisconsin's Cyber Annex is not the production of a planning document; but, rather demonstrated metrics that the state is prepared to respond to a cyber incident.

B. Organization

State Emergency Operations Center (SEOC):

1. State Emergency Operations Center is responsible for Wisconsin's interagency incident management and coordinating Federal and State Roles.

2. During an emergency or disaster situation, the Cyber Annex primary and support agencies will assign personnel to the SEOC, as appropriate. Appendix A provides a cross reference based on Critical Infrastructure Key Resource (CIKR) Sector.

3. The DOA, as the agency responsible for implementation of the Cyber Annex will respond directly to the Officer in Charge/Operations Officer in the State EOC. Alternatively, "If the governor determines that the emergency is related to computer or telecommunication systems, he or she may designate the department of administration as the lead agency to respond to that emergency."[6]

4. DMA/WEM and DOA may assign lead coordinating responsibilities to the appropriate agencies based on the physical impact of a cyber incident.

5. The SEOC will be responsible for coordination with the US DHS Unified Coordination Group (UCG.) Upon notification of a potential or actual incident, the Secretary of Homeland Security activates the appropriate Senior Officials and Staff to make up the UCG Incident management Team (IMT). The UCG IMT is tailored with required DHS components and Federal departments for a cyber incident. The USC IMT will provide subject-matter expertise related to the cyber threat, analysis, and recommendations.[7]

6. The SEOC operations will be tailored with personnel and materials from State Agencies in response to the cyber incident. The DOA/DET provides subject-matter expertise related to the cyber threat, analysis, and recommendations to the SEOC. The SEOC will be activated at one of the following SEOC levels as amended for cyber incidents:

   - Level I Full Activation. WEM, DMA/WING, DOA, WiDHS, DNR, DOT Highways, State Patrol, DATCP, DOJ/WSIC and DOC having representatives in the SEOC. Other state and federal agencies may be in the SEOC as well.

   - Level II Partial Activation. WEM, DMA/WING, DOA, WiDHS, DNR, DOT Highways, State Patrol, and DOJ/WSIC have representatives in the SEOC. Other state and federal agencies are on standby.

   - Level III Minimal Activation. ***(Optional)*** This activation is primarily intended to monitor severe weather conditions in the state. In addition to WEM staff, DOA, State Patrol and DOT Highways will be asked to

[6] Wis. Stats. § 323.10
[7] US DHS. "National Cyber Incident Response Plan" Draft version 1.2.

send a representative to the SEOC. Other state and federal agencies are on standby.

- Level IV Daily Steady State Operations. At this level a Duty Officer is on call 24 hours per day seven days per week. At this level incidents are recorded in e-sponder.

Wisconsin Cyber Response Coordination Group (WiCRCG):

1. The WiCRCG is comprised of senior representatives from federal and state agencies that have roles and responsibilities related to preventing, investigating, defending against, responding to, mitigating, and assisting in the recovery from cyber incidents and attacks. It is an operational force with human and material resources to recover from a cyber incident that will begin activation at SEOC Level III. The WiCRCG may be co-located with the SEOC; however, in most cases will be co-located with the greatest available pool of appropriate technical expertise, equipment and systems.

    - State Chief Information Officer or alternate;

    - State Chief Security Officer or alternate;

    - DOJ/WSIC Law Enforcement Liaison;

    - The State of Wisconsin Security Operations Center / Security Emergency Response team;

2. In the event of a cyber incident requires a federal response and interagency coordination, the WiCRCG is convened to harmonize operational efforts and facilitate information-sharing.

3. The WiCRCG is an interagency forum where organizations responsible for a range of activities (technical response and recovery, law enforcement, intelligence, and defensive measures) coordinate for the purposes of preparing for and executing an efficient and effective response to an incident.

4. The WiCRCG performs the following functions:

    - Provides input to member agency and department heads and the SEOC on cyber security issues, incidents, and threats;

    - Assists in reviewing threat assessments and providing strategic situational awareness and decision support across the national cyber incident management spectrum, including prevention, preparedness, response, and recovery;

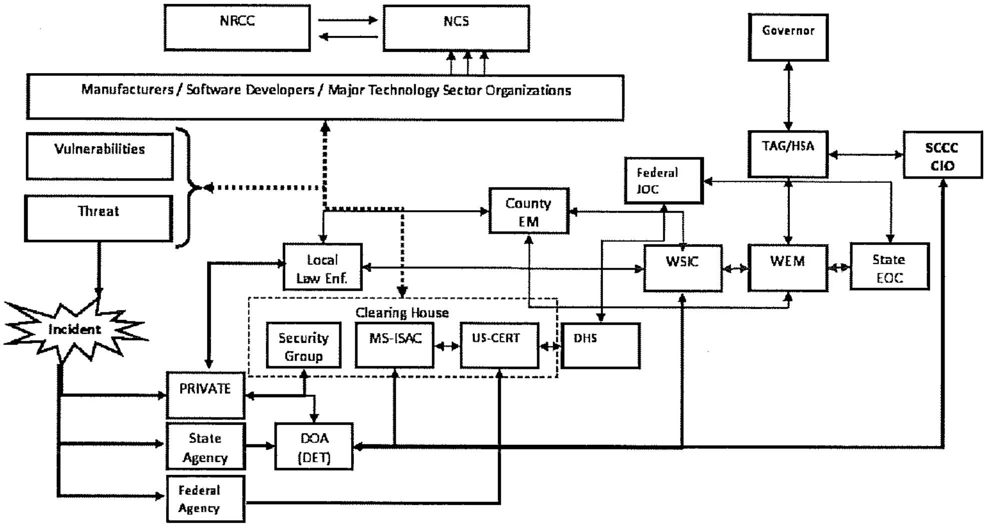
- Synthesizes information, frames policy issues, and recommends actions—including use or allocation of Federal resources—for agency and department heads, the SEOC, and other appropriate officials; and

- As appropriate, supports the Office of the Governor.

Roles and Responsibilities for Interagency Coordination.

1. A Unified Command arising from a cyber incident will be located in the Wisconsin SEOC. This recognizes that a cyber incident may not occur in isolation. "Effective unified command is indispensable to response activities and requires a clear understanding of the roles and responsibilities of each participating organization. Success requires unity of effort, which respects the chain of command of each participating organization while harnessing seamless coordination across jurisdictions in support of common objectives."[8]

2. Communications requirements during a cyber incident are complex. The following illustrates anticipated information flows.



3. NIMS guides the State and Local government response, NRF guides the Federal response.[9] A critical aspect of a cyber incident is the ability to

[8] U.S. Department of Homeland Security, *National Response Framework*, Page 10. Washington DC, January 2008.

[9] The U.S. Department of Homeland Security, National Response Plan, Cyber Incident Annex was published in December 2004, prior to the publication of NIMS in Jananuary 2008. It identifies Coordinating Agencies and Cooperating Agencies.

work effectively across organizational boundaries as primary responsibility for an cyber incident may pass between agencies. Establishment of liaison officers[10] between agencies and the private sector is critical. Within this framework Wisconsin has further identified initial cyber response. They are:

- ESF Coordinator. DMA/WEM is the ESF Coordinator and confers with DOA/DET for technical assistance and support.[11]

- Primary Agencies (P). A Cyber Annex agency is an entity with significant authorities, roles, resources, or capabilities for functions defined within the Annex. When the Cyber Annex is activated in response to an incident, the primary agency is responsible for:

  - Supporting the ESF coordinator and coordinating closely with the other primary and support agencies. See Appendix A.

  - Orchestrating support within their functional area for the State.

  - Providing staff for the operations functions at fixed and field facilities.

  - Notifying and requesting assistance from support agencies.

  - Managing mission assignments and coordinating with support agencies, as well as appropriate State officials, operations centers, and agencies.

  - Working with appropriate private-sector organizations to maximize use of all available resources.

  - Supporting and keeping other ESFs and organizational elements informed of ESF operational priorities and activities.

  - Conducting situational and periodic readiness assessments.

  - Executing contracts and procuring goods and services as needed.

  - Ensuring financial and property accountability for Cyber Annex activities.

  - Planning for short- and long-term incident management and recovery operations.

[10] The U.S. Department of Homeland Security, National Incident Management System (NIMS), December 2008 Page 50.

[11] Wis. Stat. Chapter 323.

  - Maintaining trained personnel to support interagency emergency response and support teams.

  - Identifying new equipment or capabilities required to prevent or respond to new or emerging threats and hazards, or to improve the ability to address existing threats.

- Support Agencies (S). Support agencies are those entities with specific capabilities or resources that support the primary agency in executing the Cyber Annex mission. When the Annex is activated, support agencies are responsible for:

  - Conducting operations, when requested by DHS or the designated ESF primary agency, consistent with their own authority and resources, except as directed otherwise pursuant to sections 402, 403, and 502 of the Stafford Act.

  - Participating in planning for short- and long-term incident management and recovery operations and the development of supporting operational plans, SOPs, checklists, or other job aids, in concert with existing first-responder standards.

  - Assisting in the conduct of situational assessments.

  - Furnishing available personnel, equipment, or other resource support as requested by DHS or the ESF primary agency.

  - Providing input to periodic readiness assessments.

  - Maintaining trained personnel to support interagency emergency response and support teams.

  - Identifying new equipment or capabilities required to prevent or respond to new or emerging threats and hazards, or to improve the ability to address existing threats.

4. The End User (EU) is primarily private sector entities; however, state and federal agencies may also be considered End Users and the target of a cyber incident.

   - **Supplier / Service Provider.** Private-sector entities provide response resources (donated or compensated) during an incident – including specialized teams, essential service providers, equipment, and advanced technologies – through local public-private emergency plans or mutual aid and assistance agreements, or in response to requests from government and nongovernmental-volunteer initiatives.

- **End User (Client.)** The End User equates to the NRF Impacted Organization or Infrastructure. These are organizations that may be impacted by direct or indirect consequences of the incident. These include privately owned critical infrastructure, key resources, and other private-sector entities that are significant to local, regional, and national economic recovery from the incident.

5. The following table illustrates agency roles and responsibilities across a range of Cyber incidents

	Roles Based on Category of Cyber Incident							
		System Fault (1)	Accident (2)	Disaster (3)	Crime (4)	Terrorism (5)	Act of War (6)	
	Scope:	Statewide	Statewide	Regional	Regional	National	Global	
	End User (Client)	R	R	R	A	A	A	R=Responsible
	Service Provider	R	R	R	A	A	A	A=Assists
	Manufacturer	R	R	R	A	A	A	
FED	**DHS**			**P**	S	S	S	C=Coordinator
	DOJ/FBI			S	**P**	**P**	S	P=Primary
	DoD			S	S	S	**P**	S=Supporting
WISC	**DMA/WEM**			C	C	C	C	
	DOA/DET			**P**	S	S	S	<u>Agencies:</u>
	DOJ/WSIC			S	**P**	S	S	Fed = Federal
	DMA/WING			S	S	**P**	S	Wisc = State

III. ACTIONS

A. Pre-Incident

1. DMA/WEM, DMA/WING, DOJ/WSIC and DOA/DET form the nucleus of the State of Wisconsin's pre-incident planning for cyber incidents. Each agency is responsible for on-going collaboration with their respective federal partners and other state public and private entities. The intent is to build relationship which leverage Federal and State and private sector capabilities.

2. Federal departments and agencies maintain computer incident response capabilities that can rapidly respond to cyber incidents on their networks, including events of prolonged duration. Law enforcement, the Intelligence Community, and DOD also maintain mechanisms that improve the Nation's readiness to address cyber incidents. The Department of Justice has a network of prosecutors trained in handling cybercrime. The Federal

Bureau of Investigation and the U.S. Secret Service have agents that specialize in high-tech investigations. Law enforcement's international cybercrime network enables investigators rapidly to obtain electronic data and evidence from foreign countries.

B. Notification and Activation Procedures

1. Notification of a cyber incident will be initiated through the DOJ/WSIC or the DMA/WEM Duty Officer, either of whom will ensure the DOA/DET Enterprise Help Desk is notified. Upon notification, the Wisconsin State Emergency Operation Center (SEOC) will be alerted at a level determined by the WEM Duty Officer. The Wisconsin Cyber Response Coordination Group (WiCRCG) will be alerted by the Enterprise Help Desk.

C. Resources and Potential Sources of Incident Notifiation.

- **DOJ/WSIC Bulletin.** The WSIC Intelligence Bulletin is a collaborative effort of the Wisconsin Department of Justice, Division of Criminal Investigation; U.S. Department of Justice, Federal Bureau of Investigation; Milwaukee Police Department; Wisconsin Joint Terrorism Task Force; Southeastern Wisconsin Threat Analysis Center; Eastern and the Western Districts of the U.S. Attorney's Office, and the Anti-Terrorism Advisory Council..

- **WI-ISAC Secure Portal.** This portal is a joint effort between the State of Wisconsin and the Multi-State Information Sharing and Analysis Center (MS-ISAC). The MS-ISAC is a voluntary and collaborative organization comprising all 50 States and the District of Columbia focused on raising the cyber security readiness and response in each state. The WI-ISAC will provide the following benefits to members:

  - Direct access to cyber security threat information from the State;

  - Access to security awareness materials, including computer-based training modules;

  - Access to security policy templates;

  - Access to security-related solutions at enterprise price points negotiated by the State; and,

  - Periodic meetings, teleconferences and webcasts to promote peer networking and information sharing.

- **WWW.READYWISCONSIN.GOV.** Ready Wisconsin is an initiative of Wisconsin Emergency Management designed to educate and empower Wisconsinites to prepare for and respond to all kinds of emergencies including natural disasters and potential terrorist attacks.

- **HTTP://ITSECURITY.WI.GOV.** SecurITy is an initiative of the Wisconsin Department of Administration, Division of Enterprise Technology specifically focused on cyber security education and resources for Wisconsin citizens.

1. Procedures in this annex are implemented when it is determined that a cyber-related Incident of National Significance[12] is imminent or underway. The NCRCG is convened and immediately notifies the DHS/IAIP/NCS. Notification is made through established communications channels that exist between the Federal Government, nongovernmental entities, and the public. Such channels of communication include:

- **National Cyber Alert System**: This system provides an infrastructure, managed by US¬CERT, for relaying timely and actionable computer security update and warning information to all users.

- **Homeland Security Information Network (HSIN)** Joint Regional Information Exchange System: This communications network provides States and major urban areas real-time interactive connectivity with the HSOC through a secure system carrying information on a Sensitive-but-Unclassified (SBU) level to all users.

- **National Operations Center:** This is the primary national-level hub for domestic incident management communications and operations.

- **Cyber Warning Information Network:** This network provides out-of-band (i.e., not dependent on Internet or PSTN) connectivity to government and industry participants. The network is engineered to provide a reliable and survivable network capability.

- **HSIN/US-CERT Portal**: This is a secure collaboration tool for private and public sectors to actively converse about cyber security vulnerabilities, exploits, and incidents in a trusted environment among and between members.

- **US-CERT Public Web Site:** This Web site provides the primary means for US-CERT to convey information to the public at large. The

[12] The term "Incident of National Significance" was discontinued with implementation of the NRF. It is included here as an exact quote from the Cyber Annex to the NRP.

site includes relevant and current information on cyber security issues, current cyber activity, and vulnerability resources.

D. Initial Actions following Notification

1. Following notification the following actions will be taken:

   - The SEOC and WiCRCG will establish the facts and assumptions concerning the cyber incident. This will require establishing a single liaison with private sector entities involved in the restoration of services after an incident occurs. Private sector entities will be consulted in the cyber response decision making processes.

   - SEOC and WiCRCG facts will be provided to the DOJ/WSIC and DMA/JOC who will develop National Requests for Information (RFIs) concerning response and recovery.

   - Following establishment of initial facts concerning the incident the SEOC in conjunction with the WiCRCG:

     - Recommend the SEOC operating level.

     - Provide recommendations to cabinet members in accordance with the provision of Wis. Stat. Chapter 323.

   - The SEOC and WiCRCG will cooperatively assess the on-going impacts of the incident, provides analysis of the extent and duration of incident, and identifies requirements for consequence management.

   - In coordination with federal, tribal, and local governments, SEOC will recommend prioritization of actions for the restoration of computer and network services during response and recovery operations.

2. During a significant incident, the WiCRCG may report incident information to external organizations. Reports will contain an appropriate classification based on the type of incident and clearance by the SEOC. Recipients shall agree to observe the classification. External organizations include:

   - The Multi-State Information Sharing and Analysis Center (MS-ISAC). The MS-ISAC is the channel of communication to the United States Computer Emergency Readiness Team (US-CERT) of the Department of Homeland Security.

- Wisconsin InfraGard, an FBI-sponsored group of public and private organizations sharing information related to cyber and physical security.

- IC3. Internet Crime Complaint Center (IC3). A partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C).

3. DHS/IAIP/NCSD, other elements of DHS, the Intelligence Community, FBI, DOD, and other Government agencies work closely together in the NCRCG and individually to coordinate response during a cyber incident or attack, identify those responsible, and otherwise respond appropriately.

4. When a cyber Incident of National Significance occurs, DHS/IAIP/NCSD, through the NCRCG, coordinates with the National Communications System (NCS) and supports the Joint Telecommunications Resources Board (JTRB).

5. The US-CERT Operations Center tracks potential cyber incidents and, when warranted, reports them to the NCRCG. The NCRCG notifies the HSOC of cyber-related incidents. The NCRCG, in coordination with the IIMG, makes recommendations to the Secretary of Homeland Security, who is responsible for designating Incidents of National Significance. The activities described in this annex are implemented when a cyber-related Incident of National Significance is imminent or underway.

E. Ongoing Actions

1. DMA/WEM, DOJ/WSIC, DOA/DET are working collaboratively with DHS and DOJ/FBI to develop and maintain situational awareness of the cyber domain. Cyber components are being included in sector specific exercises.

2. DHS coordinates technical and other assistance with and/or to other Federal agencies and, upon request, to the State, local, and tribal governments and the private sector for response to major failures of critical information systems. Requests for Federal assistance are handled as described in Section V of the NRP.

Challenges and Considerations

1. The response to and recovery from a cyber incident must take into account existing challenges to the effective management of significant cyber incidents and the resulting physical effects of such cyber incidents and of cyber consequences of physical incidents. Such consideration allows

resources to be appropriately channeled into resolving identified challenges. Identifiable challenges include:

- **Management of Multiple Cyber Events**: The occurrence or threat of multiple cyber incidents may significantly hamper the ability of responders to adequately manage the cyber incident. Strategic planning and exercises should be conducted to assist in addressing this problem.

- **Availability and Security of Communications:** A debilitating infrastructure attack could impede communications needed for coordinating response and recovery efforts. A secure, reliable communications system is needed to enable public and private-sector entities to coordinate efforts in the event that routine communications channels are inoperable.

- **Availability of Expertise and Surge Capacity:** Federal agencies must ensure that sufficient technical expertise is developed and maintained within the Government to address the wide range of ongoing cyber attacks and investigations. In addition, the ability to surge technical and analytical capabilities in response to cyber incidents that may occur over a prolonged period must be planned for, exercised, and maintained.

- **Coordination With the Private Sector:** Cyberspace is largely owned and operated by the private sector; therefore, the authority of the Federal Government to exert control over activities in cyberspace is limited.

APPENDIX A NOTIFICATIONS.

The following agencies will be notified based on the nature of the incident and sector involved.

Agency	Sector	Contact:
DATCP	Agriculture and Food	
DFI	Banking and Finance	
DATCP	Chemical	
DNR	Commercial Facilities	
PSC	Communications	
DWD	Critical Manufacturing	
DNG	Dams	
DWD	Defense Industrial Base	
DMA	Emergency Services	
DATCP	Energy	
DOA	Government Facilities	
DHS	Healthcare and Public Health	
DOA	Information Technology	
DNR	National Monuments and Icons	
PSC	Nuclear Reactors,	
DATCP	Materials and Waste	
DOA	Postal and Shipping	
DOT	Transportation Systems	
DNR	Water	

APPENDIX B: Authorities.

Authorities: This Cyber Annex considers the provisions of the following:

State and Federal Laws.

- PL 106-390/42 U.S.C. 5121, et seq. The Robert T. Stafford Disaster Assistance and Emergency Relief Act
- The Enhancement of Non-Federal Cyber Security, the Homeland Security Act (Section 223 of P.L. 107-276).
- Federal Information Security Management Act (FISMA).
- Section 706, Communications Act of 1934, as amended (47 U.S.C. 606).
- The Defense Production Act of 1950, as amended.
- National Security Act of 1947, as amended.
- Wisconsin Statutes Chapter 16 the Department of Administration
- Wisconsin Statutes Chapter 323: Emergency Management.

The following Executive Orders and Directives:

- Homeland Security Presidential Directive-5 (HSPD-5).
- Homeland Security Presidential Directive-7 (HSPD-7).
- Executive Order 12472: The Assignment of National Security Emergency Preparedness.
- National Security Directive 42: National Policy for the Security of National Security Telecommunications and Information Systems.
- Executive Order 12333: United States Intelligence Activities, as amended.
- Wisconsin Executive Order #7: Creation of the Wisconsin Homeland Security Council

- Wisconsin Executive Order # 81: Designation of the National Incident Management System (NIMS) as the Basis for Incident Management in the State of Wisconsin

- Wisconsin Executive Order #143: Modification of the Wisconsin Homeland Security Council. Increases Council Membership to 9.

- Wisconsin Executive Order #268: Modification the Wisconsin Homeland Security Council. Increases Council Membership to 13.[13]

The following reports and studies provide additional guidance.

- National Strategy to Secure Cyberspace (2003).

- Cyberspace Policy Review (2009).[14]

- National Cyber Incident Response Plan (Draft Version 1.2)

[13] EO 268 enabled the appointment of the Wisconsin Chief Information Officer. It references EO 143 which is included for completeness only.

[14] President Obama's 60-day comprehensive, "clean-slate" review to assess U.S. policies and structures for cyber security.

APPENDIX C: CYBER INCIDENT DEFINITIONS.

This Appendix provides emergency managers with a framework for identification of six main categories of cyber threats.

The concept of a cyber attack was first developed in a 1984[15] novel. Since that time the world has become increasingly dependent of computers and networks for all aspects of social, political and economic activity. At the same time the ability of state and non-state actors to engage in cyber attacks, with little or no support structure, has grown exponentially. A successful attack can be carried out by individual acting alone[16] or recognized terrorists organizations.[17] For a comprehensive and ongoing dialogue of Cyber attack patterns see: Common Attack Pattern Enumeration and Classification (CAPEC) at http://capec.mitre.org/.

A. System Fault (1).

1. A fault is a "condition that causes a device or system component to fail to perform in a required manner."[18] In this situation failures may be reported; however, are limited in scope. System faults range from minor errors caused by newly released software to significant network outages caused by failures at telecommunication network nodes. These include configuration errors or problems resulting from systems maintenance.[19] Faults occur in the normal steady state operations of the cyber infrastructure and are corrected by owners, operators, and suppliers of the underlying technology and do not require activation of an emergency management capability.

2. Past System Faults:

- 1993 -- Intel Pentium floating point divide. A silicon error causes Intel's highly promoted Pentium chip to make mistakes when dividing floating-point numbers that occur within a specific range. For example, dividing 4195835.0/3145727.0 yields 1.33374 instead of 1.33382, an error of 0.006 percent. Although the bug affects few users, it becomes a

[15] Gibbons, William. Neuromancer., 1984 Ace Books.

[16] Singel, Ryan. "San Francisco Held Cyber-Hostage? Disgruntled Techies Have Wreaked Worse Havoc", Wired Blog Network. July 16, 2008. < http://blog.wired.com/27bstroke6/2008/07/insider-tech-at.html> (accessed February 10, 2009)

[17] Michael Colarik, Andrew. "Chapter III - Cyber Terrorism Evolution". Cyber Terrorism: Political and Economic Implications. IGI Publishing. © 2006. Books24x7. <http://common.books24x7.com/book/id_14695/book.asp> (accessed February 4, 2009)

[18] Slade, Robert. "F ". Dictionary of Information Security. Syngress Publishing. © 2006. Books24x7. <http://common.books24x7.com/book/id_14602/book.asp> (accessed July 7, 2009)

[19] Garfinkel, Simson.. History's Worst Software Bugs. Wired Magazine. Available at: http://www.wired.com/software/coolapps/news/2005/11/69355?currentPage=1
Last Visited: July 30, 2009.

public relations nightmare. With an estimated 3 million to 5 million defective chips in circulation, at first Intel only offers to replace Pentium chips for consumers who can prove that they need high accuracy; eventually the company relents and agrees to replace the chips for anyone who complains. The bug ultimately costs Intel $475 million.

- July 2008 Apple announced that 10% of messages sent to mac.com and me.com for three days had been permanently lost.
- January 15, 1990 -- AT&T Network Outage. A bug in a new release of the software that controls AT&T's #4ESS long distance switches causes these mammoth computers to crash when they receive a specific message from one of their neighboring machines -- a message that the neighbors send out when they recover from a crash. One day a switch in New York crashes and reboots, causing its neighboring switches to crash, then their neighbors' neighbors, and so on. Soon, 114 switches are crashing and rebooting every six seconds, leaving an estimated 60 thousand people without long distance service for nine hours. The fix: engineers load the previous software release.
- 1988-1996 -- Kerberos Random Number Generator. The authors of the Kerberos security system neglect to properly "seed" the program's random number generator with a truly random seed. As a result, for eight years it is possible to trivially break into any computer that relies on Kerberos for authentication. It is unknown if this bug was ever actually exploited.

B. Accident (2).

1. An accident is anything that happens suddenly or by chance without an apparent cause. For example a car accidentally crashing into a telecommunications hotel would be an accident. Accidents range from inadvertently disabling systems to major structural damage to a facility, electrical, or telecommunications systems.[20]

- 2008 January 2008. DUBAI — An estimated 1.7 million Internet users in the UAE have been affected by the recent undersea cable damage, an expert said yesterday, quoting recent figures published by TeleGeography, an international research Web site. FLAG Europe-Asia cable 8.3km away from Alexandria, Egypt and SeaMeWe-4 affected at least 60 million users in India, 12 million in Pakistan, six million in

[20] Asma Ali Zain. Cable damage hits 1.7m Internet users in UAE. Khaleej Times Online. Available at http://www.khaleejtimes.com/DisplayArticle.asp?xfile=data/theuae/2008/February/theuae_February155.xml&section=theuae. By (Our staff reporter)

Egypt and 4.7 million in Saudi Arabia." Almost 90 per cent of Internet traffic is routed through undersea cables and only 10 per cent is done through the satellite.

C. Disaster (3).

1. The difference between accidents and disasters is magnitude. A disaster is an event that causes great loss of life and or damage. For example a tornado or flood would be considered a disaster. However, some accidents become disasters. In the case of Chernobyl an accident may become a disaster. Disasters range from damage caused by severe weather to New Madrid fault scenarios.

- April 13, 1992. Chicago underground flood. Resulted in 250 million gallons of water flooding 300 buildings in the downtown area. Some buildings had up to 40 feet of water in the lower levels. 100s of small and medium businesses suddenly cut off from their data and records

D. Crime (4).

1. A criminal event is generally characterized by the potential for illegal profit. Also criminal activities would include items such as Internet Crimes Against Children (ICAC) and "hacking."

- April 9, 2009: Fiber-optic cuts in San Carlos and San Jose near Silicon Valley shut down two IBM facilities and affected an organization in charge of Internet domain names. The cuts, in San Carlos and San Jose, California, also disrupted wired and wireless telecommunications services for thousands of users in the region.

- March 2007. TJX, the parent company of T.J. Maxx, Marshall's, and other retailers, disclosed in a Securities and Exchange Commission filing last week that more than 45 million credit and debit card numbers may have been stolen from its IT systems over an 18-month period, making it the largest customer data breach on record.

- January 24, 2003:The SQL slammer worm, also known as the Sapphire worm, attacks vulnerabilities in Microsoft SQL Server and MSDE causes widespread problems on the Internet

- Sept. 18, 2002: The Nimda worm is discovered and spreads through a variety of means including vulnerabilities in Microsoft Windows and backdoors left by Code Red II and Sadmind worm.

- August 4, 2002: A complete re-write of the Code Red worm, Code Red II begins aggressively spreading, primarily in China.

- 1995/1996 -- The Ping of Death. A lack of sanity checks and error handling in the IP fragmentation reassembly code makes it possible to crash a wide variety of operating systems by sending a malformed "ping" packet from anywhere on the internet. Most obviously affected are computers running Windows, which lock up and display the so-called "blue screen of death" when they receive these packets. But the attack also affects many Macintosh and Unix systems as well.

E. Terrorism (5).

1. Cyber Terrorism can be defined as: "The unlawful destruction, disruption, or disinformation of digital property to intimidate or coerce governments or societies in the pursuit of goals that are political, religious or ideological."[21] Terrorism includes "Hacktivism" which is "the nonviolent use of illegal or legally ambiguous digital tools in pursuit of political ends. These tools include web site defacements, redirects, denial-of-service attacks, information theft, web site parodies, virtual sit-ins, virtual sabotage, and software development."[22] Terrorism also includes the use of electronic or digital systems to achieve a kinetic effect.

- May 2007. Estonia was subjected to a mass cyber-attack in the wake of the removal of a Russian World War II war memorial from downtown Talinn. The attack was a distributed denial of service attack in which selected sites were bombarded with traffic in order to force them offline; nearly all Estonian government ministry networks as well as two major Estonian bank networks were knocked offline; in addition, the political party website of Estonia's current Prime Minister Andrus Ansip featured a counterfeit letter of apology from Ansip for removing the memorial statue. Despite speculation that the attack had been coordinated by the Russian government, Estonia's defense minister admitted he had no evidence linking cyber attacks to Russian authorities. Russia called accusations of its involvement "unfounded," and neither NATO nor European Commission experts were able to find any proof of official Russian government participation.[3] In January 2008 a man from Estonia was convicted for launching the attacks against the Estonian Reform Party website and fined.[4][5]

- May 2003. One example of cyberterrorists at work was when terrorists in Romania illegally gained access to the computers controlling the life support systems at an Antarctic research station, endangering the 58 scientists involved. However, the culprits were stopped before damage

[21] Major Bill Nelson, Cyberterror, Prospects and Implications. (Monterey, CA: Center for the Study of Terrorism and Irregular Warfare. Naval Post Graduate School, 1999)

[22] Samuel, Alexandra (August 2004), Hacktivism and the Future of Political Participation, http://www.alexandrasamuel.com/dissertation/index.html, Last visited on 2009-04-09.

actually occurred. Mostly non-political acts of sabotage have caused financial and other damage, as in a case where a disgruntled employee caused the release of untreated sewage into water in Maroochy Shire, Australia. [3] Computer viruses have degraded or shut down some non-essential systems in nuclear power plants, but this is not believed to have been a deliberate attack.

F. Act of War (6).

1. Any act occurring in the course of declared war; armed conflict, whether or not war has been declared, between two or more nations; or armed conflict between military forces of any origin. 18 U.S.C.

- August 8, 2008. Georgia's government and commercial were hit by multiple cyberattacks including denial of service and hijacking. Government sites included: the Ministry of Foreign Affairs, the Ministry of Defense, and President Mikhail Saakashvili. These sites were either blocked or traffic accessing the sites redirected to servers in Russia and Turkey. Part of the attack included the introduction of websites that appeared to be Georgia Official; however, were actually fraudulent with false information. Parliament.ge and president.gov.ge were flooded with HTTP requests and efforts to correct the misdirection were quickly countered with new re-directions.

- October 2002. "I want simultaneous, multidirectional, continuous effects: combined arms maneuver, operational fires, information operations—synchronize conventional, special operational forces(SOF) & other government agencies (OGAs)." Lieutenant General David D. McKiernan Commander, Coalition Land Component Command Operation Iraqi Freedom. The IO section planned and executed doctrinal IO missions.

Record of Changes

Table 1: Record of Changes

Change #	Date	Agency/Individual	Change
1.	4/12/2011	S. Sharpe	Note on pg 1: Changed references to 'National Response Plan' to 'National Response Framework
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			
21.			
22.			
23.			